# Table of Contents

- **Foreword**  
  By Ted Claypoole  
  xiii

- **Preface**  
  By Roland L. Trope and Thomas J. Smedinghoff  
  xv

- **Acknowledgments**  
  xxiii

- **About the Authors**  
  xxv

- **About the Editors**  
  xxxi

## PART I. INTRODUCTION

- **CHAPTER 1. The Challenge**  
  By Roland L. Trope and Thomas J. Smedinghoff  
  3

- **CHAPTER 2. The Importance of Cybersecurity Due Diligence for an M&A Deal**  
  By Roland L. Trope  
  9

  1. Cybersecurity Challenges  
  9
  2. Vulnerability of Target’s Digital Assets  
  15
  3. Vulnerability of Target’s Operations and Businesses  
  16
  4. Vulnerability of Target’s Dependency on Critical Infrastructure  
  18
  5. Contamination of the Acquirer’s Networks and Data  
  19
  6. Lessons from Recent Cyber Incidents  
  20
    6.1. Neiman Marcus  
    22
    6.2. Yahoo!  
    25
    6.3. Target Corporation  
    34
    6.4. Sony Pictures  
    35
    6.5. Volkswagen  
    36

- **CHAPTER 3. Cybersecurity Risks to an M&A Deal’s Objectives**  
  By Roland L. Trope  
  43

  1. Key Cybersecurity Risks to an M&A Transaction  
  43
  2. Premises for Planning Cybersecurity Due Diligence  
  52
CHAPTER 4. Basic Cybersecurity Concepts .............................. 55
   By Thomas J. Smedinghoff
   1. Cybersecurity ........................................ 55
   2. Digital Assets to Be Protected ........................... 58
   3. Goal of Cybersecurity .................................. 58
      3.1. Confidentiality ................................... 59
         3.1.1. Authentication .............................. 60
         3.1.2. Authorization .............................. 61
      3.2. Integrity ........................................ 61
      3.3. Availability ..................................... 62
   4. Threats Addressed by Cybersecurity ...................... 62
      4.1. Physical and Environmental Threats ................. 63
      4.2. Technical Threats ................................ 63
      4.3. People Threats ................................... 64
      4.4. Examples of Threats ................................ 64
   5. Security Controls ..................................... 67
      5.1. Categorization Based on Timing of Security Controls .... 68
      5.2. Categorization Based on Nature of Security Controls .... 68

PART II. DUE DILIGENCE:
WHAT THE ACQUIRER SHOULD KNOW

CHAPTER 5. Identification of Target’s High-Value Digital Assets ...... 73
   By Jonathan P. Adams and Matthew Staples
   1. Introduction ......................................... 73
      1.1. Subject Matter and Goals ............................ 73
      1.2. Background ....................................... 75
   2. Due Diligence Issues .................................... 75
      2.1. Identify Digital Assets ............................ 76
      2.2. Identify Storage Used ............................. 76
      2.3. Identify Control of Digital Assets .................. 77
      2.4. Have Vulnerabilities Been Identified and Addressed? .. 78
      2.5. Separation of Business Versus Operational
            Digital Assets .................................. 79
      2.6. Reliance on Internet for Communication .............. 80
      2.7. Risk Profile of Target Business Sector .............. 80
      2.8. Supply Chain Dependencies ........................ 81
      2.9. Information Sharing Activities ..................... 82
         2.9.1. Receipt of Intelligence-Sharing Reports ........ 82
         2.9.2. Receipt of Classified Cyberintelligence
                  Information .................................... 83
2.9.3. Recipient of Industrial Control Systems Cyber Emergency Response Team Alerts ............. 84
2.9.4. Recipient of DHS Notices ........................... 85
2.9.5. Participation in an ISAC ............................... 85
2.9.6. ISAC Information Coordination ........................ 86
2.9.7. DHS Technical Assistance Agreements ............. 87
2.9.8. Information Sharing Agreements ..................... 88
3. Assessment and Analysis of Results ........................ 88

CHAPTER 6. Evaluation of Internal Cybersecurity Program ............... 89
By Stuart Levi
1. Introduction ........................................... 89
   1.1. Subject Matter and Goals .......................... 89
   1.2. Background ........................................ 89
2. Due Diligence Issues ..................................... 91
   2.1. Senior Management and Board Involvement ........... 91
   2.2. Reviewing Security Programs ........................ 93
      2.2.1. Identifying the Program That Is in Place .... 94
      2.2.2. Program Responsibility .......................... 95
      2.2.3. Program Compliance with Legal Requirements .... 95
      2.2.4. Is the Program Risk-Based and Tailored to the Target’s Business? ........... 96
      2.2.5. Cybersecurity Program Resilience ................. 96
      2.2.6. Cybersecurity Program Implementation ........... 97
      2.2.7. Cybersecurity Program Updates .................... 97
      2.2.8. Third-Party Cybersecurity Assessments ......... 98
      2.2.9. Cybersecurity Statements ........................ 99
      2.2.10. Vendor Management ............................. 100
      2.2.11. Incident Response Plan .......................... 101
      2.2.12. Impact of Acquisitions .......................... 103
   2.3. Role of Standards .................................... 103
   2.4. Budget for Cybersecurity ............................. 103
3. Assessment’s Impact on the Proposed Transaction ................... 104

CHAPTER 7. Assessment of External Dependency
Cybersecurity Program ...................................... 107
By Candace Jones
1. Introduction ........................................... 107
   1.1. Subject Matter and Goals .......................... 107
   1.2. Background ........................................ 109
2. Due Diligence Issues ..................................... 110
   2.1. Inventory Third-Party Relationships ................. 110
   2.2. Vendor Governance and Management Program ........ 112
2.3. Integration of Cyber Risk into the Vendor Governance and Management Program .................. 113
2.4. Vendor Cybersecurity Assessments ................................. 115
2.5. Onboarding and Offboarding .............................................. 117
2.6. Vulnerability and Acceptance Testing ..................................... 118
2.7. Continuous Monitoring of Vendor Relationships ........................ 118
2.8. Cyber-Risk Monitoring Should Account for Risk Inherited from Vendors ......................... 119
2.9. Incident Response Procedures .............................................. 120
2.10. Target’s Obligations as Vendor— Flowdown Requirements ......................... 121
2.11. Separating the Target from Its Affiliates ................................. 121
2.12. Change Management ...................................................... 122
3. Assessment and Analysis of Results ........................................ 123

CHAPTER 8. Identifying Breaches and Assessing Incident Response Capabilities .......................... 125
By David Flint and Robert Bond
1. Introduction .................................................................................. 125
   1.1. Subject Matter and Goals ..................................................... 125
   1.2. Background .................................................................. 125
2. Due Diligence Issues ................................................................. 126
   2.1. Breach History ................................................................. 126
       2.1.1. Prior Breaches ......................................................... 126
       2.1.2. Breach Response ...................................................... 127
       2.1.3. Ongoing and Collateral Issues ................................. 128
   2.2. Preparedness for Future Breaches ........................................ 128
       2.2.1. Existence of an Incident Response Plan ...................... 129
       2.2.2. Verification and Testing of the Plan ......................... 129
       2.2.3. Expertise of Personnel ............................................. 130
       2.2.4. Training and Education .......................................... 131
   2.3. Third-Party Risk .............................................................. 131

CHAPTER 9. Evaluation of Cybersecurity Regulatory Compliance ........................................ 133
By Thomas J. Smedinghoff
1. Introduction .................................................................................. 133
   1.1. Subject Matter and Goals ..................................................... 133
   1.2. Background .................................................................. 133
2. Identifying Legal Obligations ....................................................... 136
   2.1. Statutes and Regulations ....................................................... 137
   2.2. Common Law Obligations ................................................... 138
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3. Contractual Obligations</td>
<td>138</td>
</tr>
<tr>
<td>2.4. Industry Standards</td>
<td>139</td>
</tr>
<tr>
<td>2.5. Self-Imposed Obligations</td>
<td>139</td>
</tr>
<tr>
<td>2.6. Cross-Border Issues</td>
<td>140</td>
</tr>
<tr>
<td>2.7. New Standards</td>
<td>140</td>
</tr>
<tr>
<td>3. Identifying Status of Compliance</td>
<td>141</td>
</tr>
<tr>
<td>3.1. Assessing Compliance with Laws Requiring Process-Oriented Approach</td>
<td>141</td>
</tr>
<tr>
<td>3.1.1. Written Security Program</td>
<td>142</td>
</tr>
<tr>
<td>3.1.2. Identification of High-Value Digital Assets</td>
<td>143</td>
</tr>
<tr>
<td>3.1.3. Periodic Risk Assessment</td>
<td>143</td>
</tr>
<tr>
<td>3.1.4. Implementation of Security Controls</td>
<td>144</td>
</tr>
<tr>
<td>3.1.4.A Are the Security Controls Responsive to the Risks the Target Faces?</td>
<td>144</td>
</tr>
<tr>
<td>3.1.4.B Do the Security Measures Address the Required Security Controls?</td>
<td>144</td>
</tr>
<tr>
<td>3.1.5. Regular Monitoring and Testing of Target’s Security Controls</td>
<td>147</td>
</tr>
<tr>
<td>3.1.6. Regular Review and Adjustment of Target’s Security Program</td>
<td>147</td>
</tr>
<tr>
<td>3.1.7. Oversight of Third-Party Service Provider Arrangements</td>
<td>148</td>
</tr>
<tr>
<td>3.2. Assessing Compliance with Laws Requiring Specific Security Controls</td>
<td>149</td>
</tr>
<tr>
<td>3.3. Successor Liability</td>
<td>150</td>
</tr>
</tbody>
</table>

**CHAPTER 10. Special Issues in Cybersecurity Due Diligence: Resilience and Reviews by CFIUS**

By Roland L. Trope

1. Resilience                                                           | 152  |
   1.1. Subject Matter and Background                                    | 152  |
   1.1.1. Example: Resilience of Bulk Power System Enterprises         | 155  |
   1.1.2. Example: Resilience of Financial Services Enterprises        | 157  |
   1.2. Due Diligence Issues                                            | 161  |

2. Reviews of “Covered Transactions” by CFIUS                          | 167  |
   2.1. Subject Matter and Background                                    | 167  |
   2.2. Due Diligence Issues                                            | 170  |
PART III. IMPACT OF DUE DILIGENCE ON THE PROPOSED TRANSACTION

CHAPTER 11. Addressing Risks Identified in Due Diligence . . . . . . . . . .177
By Jonathan P. Adams and Matthew Staples
1. Subject Matter and Goals ..............................................177
2. Problems That Could Emerge in Diligence ......................178
   2.1. Insufficient Ability to Assess Cybersecurity Risk .........178
       2.1.1. Desired Documentation or Information Is Missing ....179
       2.1.2. Desired Documentation Does Not Exist ............180
       2.1.3. Shifting Regulatory and Legal Environments ...181
   2.2. Serious Shortcomings in Target’s Practices or Legal Risks 181
       2.2.1. Poor Practices or Weak Policies on Information Security 182
       2.2.2. Compliance Failures ........................................182
       2.2.3. Contractual Breaches .....................................183
       2.2.4. Data Breaches and Cyber Attacks .....................184
       2.2.5. Government Investigations .............................186
       2.2.6. Litigation and Prelitigation Activity .................187
   2.3. “What You See Versus What You Hear”: Discrepancies between Documentation and Target Narratives 188
   2.4. Assessing Target’s Resilience to Cyber Threats and Attacks 188
   2.5. Review and Assessment of Findings and Report by Cybersecurity Specialist 190
3. Recourse Available to Acquirer ........................................191
   3.1. Limiting Exposure in the Underlying Agreement .........191
       3.1.1. Indemnification ..............................................192
       3.1.2. Covenants ..................................................193
       3.1.3. Closing Conditions ........................................194
       3.1.4. Purchase-Price Adjustment ..............................195
   3.2. Limiting Exposure in the Disclosure Schedules ............196

CHAPTER 12. Representations and Warranties in M&A Agreements ...............201
By William R. Denny
1. Goals of Cybersecurity Representations and Warranties ........202
2. Representation and Warranty Issues ...............................202
3. Common Cybersecurity Representations and Warranties ......204
   3.1. Compliance with Data Security Policies .................204